Restrictions on employers’ handling of criminal records information: privacy and confidentiality issues

Associate Professor Moira Paterson MONASH UNIVERSITY

The practice of criminal records checking raises a number of important issues which are highlighted in a recently updated set of guidelines issued by the Australian Human Rights Commission (AHRC). These guidelines, which were initially prepared in 2005 in response to concerns arising from a significant number of complaints alleging employment discrimination of the grounds of criminal record, focus primarily on discrimination but they also refer to broader privacy and confidentiality concerns. These issues are important as they are relevant to decisions whether to collect criminal records information and, if so, whether to retain it after the completion of employment decision-making.

Obligations arising under privacy laws

Privacy statutes in Australia

Privacy laws exist in all Australian jurisdictions except for SA and WA. The state and territory laws apply to public sector bodies in those jurisdictions, while the Commonwealth Privacy Act applies to the Commonwealth and ACT public sector and to those private sector bodies that do not fall within the small business operator exemption. The focus of this article is on the National Privacy Principles (NPPs) which regulate the private sector. It should be noted that the government has recently introduced into parliament an amending Bill which replaces the NPPs with a set of Australian Privacy Principles (APPs) which apply also to Commonwealth government agencies. However, this does not affect the specific features outlined below.

NPPs: application

The NPPs do not apply in respect of acts and practices of employers in respect of information relating to their employment relationship with current or former employees, and are therefore relevant only to the handling of criminal records information about prospective employees. In consequence, the collection of criminal records information affects private sector employers only to the extent that they have a gross annual turnover of more than $3 million (or are excluded from the small business operator exemption, for example, because they provide health services) and then only in respect of prospective employees. However, employers should bear in mind that the Australian Law Reform Commission (ALRC) has recommended that both the small business operator and the employee record exceptions should be removed from the Act. It is possible therefore that these provisions will apply more widely in the future. Further, as stated by the AHRC:

It is best practice for employers to follow privacy principles as closely as possible when dealing with information relating to a person’s criminal record. Breaches of privacy in relation to criminal record can complicate relations between an employee and employer, and may lead to claims of discrimination.

The NPPs, to the extent that they are applicable, require compliance with privacy principles which regulate the handling of identifiable personal information. They impose limitations on the collection, use and disclosure of such information and also additional requirements, including requirement to keep information secure, to keep it accurate and up-to-date and to delete it when no longer required.

NPPs relevant to criminal record information

There are two privacy principles which regulate the collection of criminal records information. The collection limitation principle in NPP 1 imposes some general limitations on the manner in which identifiable personal information is collected. These include requirements that information must be collected by “lawful and fair means”, that it must, if practicable, be collected only from the individual to whom it relates and that the individual must be informed about specific matters including the fact that his or her information has been collected. In addition, NPP 10 imposes further restrictions on the collection of “sensitive information”, including information about an individual’s criminal record. Unless the collection of that information is required by law, it cannot be collected without the individual’s consent.

Employment Law Bulletin

November/December 2012

120
These principles are unproblematic in respect of information collection from official sources as this requires the express consent of the individual concerned. However, they do impose important constraints on an employers’ collection of information in other ways (for example, via websites which provide criminal records searches). Such collection is permissible only with the consent of the individual concerned, which means that employers who are bound by the NPPs are precluded from using such sources to gather information about prospective employees except with their consent. Collection from non-official sources may also be contrary to the law to the extent that it contravenes any applicable spent convictions law as discussed further below.

**Can criminal record information be further use or disclosed and should it be destroyed?**

Also of direct relevance are the use and disclosure limitations in NPP 2 and the associated requirement in NPP 4 to take reasonable steps to destroy or permanently de-identify any information that is no longer needed for any of the purposes for which it may be used or disclosed. Subject to some exceptions that are unlikely to be of relevance to an employer’s collection of criminal records information, NPP 2 states that personal information collected must not be used or disclosed for a purpose other than the purpose for which it was collected without the individual’s consent, unless the purpose is related to the primary purpose of collection and is one which the individual would reasonably expect.

This principle is unproblematic to the extent that information is used for the purpose of considering whether or not to employ an individual, but it requires careful consideration when deciding whether or not to retain it beyond that point. Whether or not it is appropriate to retain the information depends on whether there are any further purposes related to that purpose that might reasonably be expected by the individual concerned. Thus, there may be an arguable case for retaining information about an individual’s conviction for the purposes of being able to impose appropriate supervision arrangements relevant to his or her criminal history. However, the position might be different in relation to an old conviction that is unrelated to the performance of that individual’s employment duties. It would also be different if it is decided not to employ that individual.

In general terms, it is good practice not to retain any personal information for any longer than required as this removes any further privacy requirements, including the requirement to keep it secure and up-to-date.

**The relevance of spent convictions: when can an employee lawfully not disclose a conviction to the employer?**

Legislative spent convictions regimes exist in all Australian jurisdictions other than Victoria and provide partial protection for older, less serious offences. They apply to offences that are more than 10 years old (or five years old in the case of offences committed by juveniles) and carry low maximum jail terms (in most states these vary from six to 30 months). In WA, there is a two-part regime which provides for different procedures for offences carrying a maximum jail term of 12 months and other more serious offences. Victoria instead has an administrative regime which operates to restrict disclosure of criminal records information by police but does not confer any legally enforceable rights or obligations. Except in WA, where ex-offenders must apply for certificates before their convictions can qualify as exempt, convictions become spent automatically when they meet the required criteria.

**Effect of “spent” conviction for employer and employee**

The effect of a conviction becoming spent is that there is no obligation on the ex-offender to disclose it and it is also generally permissible to disregard it for the purposes of obligations relating to disclosure of criminal history information. In addition, subject to some exceptions, spent convictions laws forbid employers and others from taking into account spent convictions in making assessments about character and fitness. A number also criminalise and/or forbid other specified dealings with criminal records (such as threaten to disclose or to fraudulently or dishonestly obtain spent convictions information from an official record).

**Liability at common law**

As noted by the AHRC, the handling of criminal records information may also potentially expose employers to potential claims under common law for breaches of privacy and wrongful disclosure of confidential information.

**Breach of confidential information**

Obligations of confidentiality are more likely to be relevant where the information is collected directly from the individual concerned. To sue for breach of confidence, a plaintiff must establish that the information in question was confidential in nature, that it was imparted on the understanding that it would be treated as confidential, and that it has been disclosed inconsistently with that obligation and to the detriment of the plaintiff.

The requirement that information is confidential in nature generally requires consideration of the extent to which it has been kept secret or not in the public domain. While an individual’s convictions are a matter of public record, it is arguable that they possess the necessary quality of confidence to the extent that they are not generally well known and that their disclosure will
generally result in some detriment to the individual to whom they relate. The requirement that information must be imparted on the understanding that it will be treated as confidential does not require that there must be any express discussion or stipulation; the obligation may be inferred from the circumstances.

The issue has yet to be judicially considered but it is arguable that the very sensitive nature of information coupled with the context in which it is gathered (that is, the specific context of employment decision-making) may create a reasonable inference that it is provided in confidence by the prospective employee to the employer for that purpose and that it is not to be disclosed for other purpose(s). In cases where the documentation relating to the employment application is headed “private and confidential”, the obligation will be more explicit. That is also the case where criminal records information is disclosed in an interview context and the applicant has been informed that the interview is confidential or words to that effect.

This may be significant in such circumstances where the employer decides to engage the applicant as an employee. For example, the employer may not disclose to other employees within the workplace information about that new employee’s record; or to another employer when that employee is seeking a reference.

Breach of privacy

The position regarding common law liability for breach of privacy remains less clear, given the absence of any decision by a higher court, which has found in favour of a plaintiff on the basis of breach of privacy, despite the fact that the High Court has cleared the way for the development of a privacy-based right of action (as occurred elsewhere, including in the UK and New Zealand). Further, there is some New Zealand authority for the proposition that the disclosure of criminal records information can raise serious privacy issues. It should also be noted that the ALRC has recommended the enactment of a statutory privacy tort.

Conclusion

While there may be good reasons (and even positive obligations) for employers to conduct criminal records checking, they should also be aware of the possible legal obligations that this may create. These can generally be minimised by conducting criminal records checks only where appropriate and minimising the retention of any information collected once employment decision-making has been completed. Employers who are bound by the Privacy Act need to bear in mind that they are bound by the NPPs in respect of their handling of information about employees who are ultimately appointed for the period pending their appointment.

Legal risks can also be reduced by complying with the best practice as outlined by the AHRC and, in particular, its recommendations that criminal record checks should only be conducted with the written consent of the job applicant or current employee and that information about a person’s criminal record should always be stored in a private and confidential manner, and used only for the purpose for which it is intended.

Moira Paterson
Associate Professor, Faculty of Law
Monash University
moira.paterson@monash.edu

About the author

Moira has published extensively on privacy related topics, including spent convictions laws. She is a member of the Privacy Advisory Committee to the Office of the Australian Information Commissioner and is admitted to practise as a barrister and solicitor in Victoria.

Footnotes

1. The author acknowledges the helpful comments of the anonymous referee. Research for this article was supported by an Australian Research Council grant. See: www.law.monash.edu.au.
3. Above, n 2 at p 7.
4. Privacy Act 1988 (Cth), Privacy and Personal Information Protection Act 1998 (NSW); Northern Territory Information Act 2002 (NT); Information Privacy Act 2009 (Qld); Personal Information and Protection Act 2004 (Tas); and Information Privacy Act 2000 (Vic). In the case of the ACT, the Commonwealth Act applies to ACT government agencies. South Australia has an administrative regime based on a set of IPPs: see, www.legislation.sa.gov.au. The Information Privacy Bill 2007 (WA) currently remains before the WA parliament.
5. The NPPs can be accessed at the Office for the Australian Information Commissioner website: www.privacy.gov.au.
6. Privacy Amendment (Enhancing Privacy Protection) Bill 2012.
7. Privacy Act 1988, s 7B(3).
8. Privacy Act 1988, s 6D.
10. Above, n 2 at p 11–12.

12. The equivalent requirement are in APP 3, as found in the Privacy Amendment Bill, n 6.

13. The equivalent requirement are also in APP 3, as found in the Privacy Amendment Bill, n 6.

14. Use and disclosure limitations are contained in APP 6, as found in the Privacy Amendment Bill, n 6.

15. The equivalent requirement are in APP 1, as found in the Privacy Amendment Bill, n 6.


18. ACT, NSW, NT and Tasmania.


21. These include exceptions for access and use by courts or police or in relation to screening checks for specific public appointments, as well as for employment involving children and other vulnerable groups: see, for example, Spent Convictions Act 2000 (ACT) s 19 and Criminal Records Act 1991 (NSW) Pt 3 Div 2 — Exclusions.

22. See, for example, the Annulled Convictions Act 2003 (Tas), s 11.

23. See, for example, the Annulled Convictions Act 2003 (Tas), s 12, and Spent Convictions Act 2000 (ACT), s 18.


25. But note that any person who receives information as a result of another’s breach of confidence may be restrained from using or disclosing the information once he or she has notice of the breach: Fraser v Evans [1969] 1 QB 349; [1969] 1 All ER 8; [1968] 3 WLR 1172.


29. Tucker v News Media Ownership Ltd [1986] 2 NZLR 716. In that case, the applicant obtained preliminary relief to restrain the public broadcast of information about his 20 year old convictions for various offences, including indecent assault.


31. Above, n 2, recommendation 5.

32. Above, n 2, recommendation 6.